REMARKS

Applicants request favorable reconsideration and allowance of this application in view of the foregoing amendments and the following remarks.

Claims 1-2, 4, 5, 7-14, 16, 17, and 19-36 are pending in this application, with Claims 1, 13, 27, and 32 being independent. Claims 6, 18, 37 and 38 have been cancelled herein without prejudice to or disclaimer of the subject matter presented therein.

Claims 1, 2, 4-5, 11, 13-14, 16-17, 25, 27-28, 30-33, 35 and 36 have been amended. Applicants submit that support for the amendments can be found in the original disclosure, and therefore no new matter has been added. Applicants further submit that the amendments, particularly those to the independent claims, are intended to avoid language such as "adapted to" that is sometimes disfavored in U.S. practice, and the amendments are not intended to substantively narrow the scope of the claims.

The Abstract and Summary of the Invention have been amended to conform with the pending claims.

Claim 36 was objected to for depending on a subsequent claim. That claim has been amended to depend only from preceding claims. Accordingly, reconsideration and withdrawal of the objection are requested.

Claims 1, 2, 4-14, 16-37 and 38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kondoh et al. (U.S. Patent 6,968,058) in view of Kobayashi et al. (U.S. Patent 7,124,094). Applicants respectfully traverse this rejection for the reasons discussed below.

As recited in independent Claim 1, the present invention includes, *inter alia*, the features of a first verification data generation unit which generates first verification data from image data using first information and not using public key cryptography, and a second verification data

generation unit which generates second verification data from image data using second information and public key cryptography, if a first verification unit verifies that the image data is not altered. Applicants submit that the cited art fails to disclose or suggest at least these features for the reasons discussed below.

Kondoh et al. discloses an image verification system that uses public key cryptography, and the Examiner correctly notes in the Office Action that Kondoh et al. does not show a first verification data generation unit not using public key cryptography. However, the Examiner asserts that Kobayashi et al. renders that feature obvious. In particular, the Examiner asserts that it would have been obvious to substitute the common key encryption system taught by Kobayashi et al. for the public key cryptography system used by Kondoh et al. because processing speed is higher for the common key encryption system when an amount of image data is large. Applicants respectfully submit that there are at least three reasons that it would not have been obvious to make the Examiner's suggested substitution.

First, Kobayashi et al. discloses the use of a common key encryption system for encoding *image* data, not for generating *verification* data. Thus, Applicants submit that one skilled in the art would not be motivated to substitute an encoding technique touted for encoding image data for one being used to generate verification data. Moreover, verification data does not necessarily involve a large amount of data, and therefore the purported advantage of the common key encryption system (faster processing for a large amount of image data) would not apply and therefore would not be a reason to make the suggested substitution.

Second, Applicants submit that using a common key encryption system would be contrary to the intended purpose of Kondoh et al. Specifically, the purpose of the system in Kondoh et al. is to provide a digital evidentiary camera system such that images captured with a digital camera

can be used as evidence with a high degree of confidence that they have not been altered. The image is encrypted with a private key when captured, and the image can later be decrypted using the public key. Access to the private key must be strictly managed, but the public key can be made public because it is very difficult to obtain the private key from knowing the public key. (See col. 1, lines 8-40) More specifically, Kondoh et al. states "the encryption key for generating the alteration detection data must never leak to third parties including the camera user." (See col. 5, lines 46-52) In contrast, a common key encryption system requires the use of the same common secret key for encrypting and decrypting, and therefore it requires transmission and/or sharing of the common secret key. Accordingly, Applicants submit that use of a common key encryption system would be inconsistent with the intent of Kondoh et al. that the encryption key be maintained strictly secret, even from the camera user. Therefore, one skilled in the art would not be inclined to substitute the common key encryption system for the public key cryptography in Kondoh et al.

Third, the invention recited in Claim 1 involves a first verification data generation unit which generates first verification data not using public key cryptography, and a second verification data generation unit which generates second verification data using public key cryptography. Thus, the invention of that claim uses a combination of units that use public key cryptography and do not use public key cryptography. However, assuming, *arguendo*, one skilled in the art were going to make the suggested substitution of the common key encryption system of Kobayashi et al. for the public key encryption system of Kondoh et al., then Applicants submit that the substitution would be made for all the public key cryptography in Kondoh et al. Hence, Applicants submit that the result would be a system using only common key encryption rather than a system, as recited in Claim 1, having a first verification data generation unit not

using public key cryptography and a second verification data generation unit using public key cryptography.

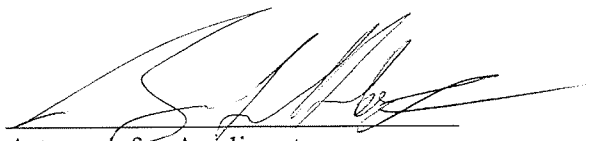
For all of the above reasons, Applicants submit that the present invention recited in Claim 1 would not have been obvious over the cited art and instead is patentable over such art.

The other independent claims recite features similar to some of those of Claim 1 discussed above, and those claims are believed to be patentable for reasons similar to Claim 1. The dependent claims are believed to be patentable for at least the same reasons as the independent claims, as well as for the additional features they recite.

In view of the foregoing, Applicants submit that the present application is in condition for allowance. An early Notice of Allowance is requested.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicants
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/lcw

FCHS_WS 1410663_1.DOC